COLLOQUIUM MATHEMATICUM

VOL. LXVII 1994 FASC. 1

NOTE ON THE GALOIS MODULE STRUCTURE OF QUADRATIC EXTENSIONS

BY

GÜNTER LETTL (GRAZ)

In this note we will determine the associated order of relative extensions of algebraic number fields, which are cyclic of prime order p, assuming that the ground field is linearly disjoint to the pth cyclotomic field, $\mathbb{Q}^{(p)}$. For quadratic extensions we will furthermore characterize when the ring of integers of the extension field is free over the associated order. All our proofs are quite elementary. As an application, we will determine the Galois module structure of $\mathbb{Q}^{(n)}/\mathbb{Q}^{(n)^+}$.

I. Let L/K be a finite Galois extension of algebraic number fields with Galois group Γ, and denote the ring of integers of K (resp. L) by $\mathfrak{o}$ (resp. $\mathfrak{O}$). Then the associated order of L/K is defined by

$$\mathcal{A}_{L/K} = \{\alpha \in K\Gamma \mid \alpha\,\mathfrak{O} \subset \mathfrak{O}\},$$

where the group algebra $K\Gamma$ operates on the additive structure of L. To determine the Galois module structure of $\mathfrak{O}$ with respect to K means to describe $\mathfrak{O}$ as a module over $\mathcal{A}_{L/K}$. One is especially interested in the question whether $\mathfrak{O}$ is free over $\mathcal{A}_{L/K}$ (i.e. $\mathfrak{O} \simeq \mathcal{A}_{L/K}$). For more details about this subject, consult [2, 5, 6].

Let us now suppose that $\Gamma = \langle\sigma\rangle$ is cyclic of prime order p with generator σ and $[K(\zeta_p) : K] = \varphi(p)$, where ζ_p is a root of unity of order p and φ denotes Euler's totient function. Since Γ is abelian, there is a unique maximal order $\mathcal{M} \subset K\Gamma$. With our additional assumption on K, the only primitive idempotents of $K\Gamma$ are $\varepsilon = \frac{1}{p}\sum_{j=0}^{p-1}\sigma^j$ and $1-\varepsilon$, so

$$\mathcal{M} = \mathfrak{o}\Gamma\varepsilon \oplus \mathfrak{o}\Gamma(1-\varepsilon) = \mathfrak{o}\varepsilon \oplus \mathfrak{o}(1-\varepsilon) \oplus \mathfrak{o}(\sigma-\varepsilon) \oplus \ldots \oplus \mathfrak{o}(\sigma^{p-2}-\varepsilon).$$

Let $\mathfrak{D}_{L/K}$ denote the different of L/K and $\mathfrak{a} \lhd \mathfrak{o}$ be minimal such that

$$\mathfrak{a}\mathfrak{O} \supset \mathfrak{D}_{L/K} + p\mathfrak{O}.$$

1991 *Mathematics Subject Classification*: Primary 11R33.

This paper was written while the author was visiting the University of Debrecen, Hungary. Many thanks to Prof. A. Pethö and the Mathematical Institute for their kind hospitality.

From the well known description of the different (see e.g. [4], Theorem 4.8) one deduces that $\mathfrak{a} = \mathfrak{o}$ if and only if L/K is at most tamely ramified.

Let $\mathrm{Tr}_{L/K}$ denote the trace from L to K.

PROPOSITION 1. *Let the notation be as above.*

(i) *The associated order of L/K is given by*

$$\mathcal{A}_{L/K} = \Big\{ a_0\varepsilon + \sum_{j=1}^{p-1} a_j(\varepsilon - \sigma^{j-1}) \;\Big|\; a_j \in \mathfrak{o} \text{ and } \sum_{j=0}^{p-1} a_j \in p\mathfrak{a}^{-1} \Big\}.$$

(ii) *If $\mathfrak{O} \simeq \mathcal{A}_{L/K}$, then $\mathfrak{a}$ is a principal ideal. Moreover, if $x \in \mathfrak{O}$ and $t \in \mathfrak{o}$ with $\mathfrak{O} = \mathcal{A}_{L/K}\, x$ and $\mathfrak{a} = t\mathfrak{o}$, then $\mathrm{Tr}_{L/K}(x/t)$ is a unit in $\mathfrak{o}$.*

(iii) *If $\mathfrak{a} = t\mathfrak{o}$ is principal, then*

$$\mathcal{A}_{L/K} = \mathfrak{o}\Gamma\left[\frac{p}{t}\varepsilon\right] = \mathfrak{o}\Gamma + \mathfrak{o}\Gamma\frac{p}{t}\varepsilon = \bigoplus_{j=0}^{p-2} \mathfrak{o}\sigma^j \oplus \mathfrak{o}\frac{p}{t}\varepsilon. \tag{1}$$

Proof. (i) Obviously, $\mathfrak{o}\Gamma \subset \mathcal{A}_{L/K} \subset \mathcal{M}$. Let $\alpha = a_0\varepsilon + \sum_{j=1}^{p-1} a_j(\varepsilon - \sigma^{j-1}) \in \mathcal{M}$ be given with $a_j \in \mathfrak{o}$. Then $\alpha \in \mathcal{A}_{L/K}$ if and only if

$$\mathrm{Tr}_{L/K}\left(\left(\frac{1}{p}\sum_{j=0}^{p-1} a_j\right)x\right) \in \mathfrak{O}$$

for all $x \in \mathfrak{O}$. This is equivalent to $\frac{1}{p}\sum_{j=0}^{p-1} a_j \in \mathfrak{D}_{L/K}^{-1}$. Since $p\mathfrak{O} + \mathcal{D}_{L/K} \subset p(\sum_{j=0}^{p-1} a_j)^{-1}\mathfrak{O}$ and by the minimality of $\mathfrak{a}$, this holds if and only if $\sum_{j=0}^{p-1} a_j \in p\mathfrak{a}^{-1}$.

(ii) Let $x \in \mathfrak{O}$ with $\mathfrak{O} = \mathcal{A}_{L/K}x$. Thus there exists an $\alpha \in \mathcal{A}_{L/K}$ with $1 = \alpha x$, and by part (i), $\alpha = a_0\varepsilon + \sum_{j=1}^{p-1} a_j(\varepsilon - \sigma^{j-1})$ with $a_j \in \mathfrak{o}$ and $\sum_{j=0}^{p-1} a_j = b \in p\mathfrak{a}^{-1}$. This yields

$$1 = \frac{b}{p}\mathrm{Tr}_{L/K}(x) - \sum_{j=1}^{p-1} a_j\sigma^{j-1}(x). \tag{2}$$

Since $L = K \otimes_{\mathfrak{o}} \mathfrak{O} = K \otimes_{\mathfrak{o}} (\mathcal{A}_{L/K}x) = K\Gamma x$, the conjugates of x are linearly independent over K. Thus we can derive from (2) that $a_j = 0$ for all $1 \le j \le p-1$ and

$$1 = \frac{b}{p}\mathrm{Tr}_{L/K}(x). \tag{3}$$

Suppose that $b\mathfrak{o} \subsetneq p\mathfrak{a}^{-1}$. Then there exist a prime ideal $\mathfrak{q} \lhd \mathfrak{o}$ with $b\mathfrak{o} \subset p\mathfrak{a}^{-1}\mathfrak{q}$ and a $\overline{b} \in p\mathfrak{a}^{-1} \setminus p\mathfrak{a}^{-1}\mathfrak{q}$. But then $(\overline{b}/p)\mathrm{Tr}_{L/K}(x) = \overline{b}/b$ is not integral, contradicting $\overline{b}\varepsilon \in \mathcal{A}_{L/K}$. Thus we have proved $b\mathfrak{o} = p\mathfrak{a}^{-1}$, which implies that $\mathfrak{a} = (p/b)\mathfrak{o}$ is principal. The second assertion of (ii) follows now from (3).

(iii) Assuming $\mathfrak{a} = t\mathfrak{o}$ and putting $\sum_{j=0}^{p-1} a_j = (p/t)b$ with some $b \in \mathfrak{o}$, this assertion is easily verified.

If L/K is at most tamely ramified (so $\mathfrak{a} = \mathfrak{o}$), Proposition 1(iii) yields $\mathcal{A}_{L/K} = \mathfrak{o}\Gamma$, which is of course well known. But furthermore, parts (ii) and (iii) of the above proposition yield also for wildly ramified extensions the following

COROLLARY. *If $\mathfrak{O} \simeq \mathcal{A}_{L/K}$, then $\mathfrak{O}$ is a free $\mathfrak{o}$-module of rank p.*

II. Now we consider the quadratic case, i.e. $p = 2$. In this case we can extend Proposition 1 to obtain a full characterization for $\mathfrak{O} \simeq \mathcal{A}_{L/K}$. Our results should be compared with Theorems 4.1 and 6.1 in [3], where this problem is considered under the additional conditions that L is an extension with given Galois group (of order 4 or 8) over some subfield $k \subset K$, the class number of k equals 1 and L/K is at most tamely ramified.

PROPOSITION 2. *Let L/K be a quadratic extension of number fields. Then the following statements are equivalent*:

(i) $\mathfrak{O} \simeq \mathcal{A}_{L/K}$.

(ii) *There exist $t, x \in \mathfrak{O}$ with $t \mid 2$, $\mathcal{A}_{L/K} = \mathfrak{o}\Gamma[(1+\sigma)/t]$ and $\mathfrak{O} = \mathcal{A}_{L/K}x$.*

(iii) *There exist $t, x \in \mathfrak{O}$ with $t \mid 2$ such that $\mathrm{Tr}_{L/K}(x/t)$ is a unit in $\mathfrak{o}$ and $\mathfrak{O} = \mathfrak{o}[x]$.*

P r o o f. The equivalence of (i) and (ii) follows from Proposition 1.

For $p = 2$, (1) yields

$$\mathfrak{o}\Gamma\left[\frac{1+\sigma}{t}\right] = \mathfrak{o} \oplus \mathfrak{o}\frac{1+\sigma}{t}. \tag{4}$$

Assume (ii). Proposition 1(ii) shows that $\mathrm{Tr}_{L/K}(x/t)$ is a unit, and together with (4) we obtain $\mathfrak{O} = \mathfrak{o}x + \mathfrak{o}\mathrm{Tr}_{L/K}(x/t) = \mathfrak{o}[x]$.

Now assume (iii). Using (4) yields $\mathfrak{O} = \mathfrak{o}[x] = \mathfrak{o}x \oplus \mathfrak{o}\mathrm{Tr}_{L/K}(x/t) = \mathfrak{o}\Gamma[(1+\sigma)/t]x$, which proves (ii).

With $t = 1$, Proposition 2 immediately yields the following

COROLLARY. *Let L/K be a quadratic extension of number fields which is at most tamely ramified. Then $\mathfrak{O} \simeq \mathcal{A}_{L/K}$ $(= \mathfrak{o}\Gamma)$ if and only if there exists an $x \in \mathfrak{O}$ such that $\mathfrak{O} = \mathfrak{o}[x]$ and $\mathrm{Tr}_{L/K}(x)$ is a unit in $\mathfrak{o}$.*

III. We will use Proposition 2 to describe the Galois module structure of cyclotomic fields over their maximal real subfield. In all cases the ring of integers turns out to be free over the associated order.

Let $3 \le n \in \mathbb{N}$ with $n \not\equiv 2 \pmod 4$, and ζ be a root of unity of order n. Put $L = \mathbb{Q}^{(n)} = \mathbb{Q}(\zeta)$ and $K = L^+ = \mathbb{Q}(\zeta + \zeta^{-1})$.

PROPOSITION 3. (i) *If $n \ne 4p^\alpha$ with $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}_0$, then*

$$\mathfrak{O} = \mathfrak{o}\Gamma\zeta.$$

(ii) *If $n = 4p^\alpha$ with $2 \ne p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$, then*

$$\mathfrak{O} = \mathfrak{o}\Gamma(1+\zeta).$$

(iii) *If $n = 2^k$ with $k \ge 2$, let $t \in \mathfrak{o}$ be a generator of the prime ideal dividing 2. Then*

$$\mathcal{A}_{L/K} = \mathfrak{o}\Gamma\left[\frac{1+\sigma}{t}\right] \quad \text{and} \quad \mathfrak{O} = \begin{cases} \mathcal{A}_{L/K}\,\zeta & \text{if } k \ge 3, \\ \mathcal{A}_{L/K}\,(1+\zeta) & \text{if } k = 2. \end{cases}$$

Proof. We always have $\mathfrak{O} = \mathfrak{o}[\zeta] = \mathfrak{o}[1+\zeta]$.

Now, $\mathrm{Tr}_{L/K}\zeta = \zeta + \zeta^{-1} = \zeta^{-1}(1-(-\zeta^2))$ is a unit in $\mathfrak{o}$ if $n \ne 4\,p^\alpha$ ($p \in \mathbb{P}$, $\alpha \in \mathbb{N}_0$), and generates the prime ideal dividing 2 in $\mathfrak{o}$ for $n = 2^k$ ($k \ge 3$). Thus Proposition 2 yields (i) and (iii) for $k \ge 3$.

For $n = 4$, $\mathrm{Tr}_{L/K}(1+\zeta) = 2$, which completes the proof of (iii).

Finally, $\mathrm{Tr}_{L/K}(1+\zeta) = 2 + \zeta + \zeta^{-1} = (1+\zeta)(1+\zeta^{-1})$ is a unit in $\mathfrak{o}$ if $n = 4p^\alpha$ with $2 \ne p \in \mathbb{P}$ and $\alpha \ge 1$, which yields (ii).

Remark. In the same way, Proposition 2 yields for $n = 2^k$ with $k \ge 3$:

(i) for $K = \mathbb{Q}(\zeta - \zeta^{-1})$:

$$\mathfrak{O} = \mathfrak{o}\Gamma\left[\frac{1+\sigma}{t}\right]\zeta$$

with t as in Proposition 3(iii);

(ii) for $K = \mathbb{Q}(\zeta^2)$:

$$\mathfrak{O} = \mathfrak{o}\Gamma\left[\frac{1+\sigma}{2}\right](1+\zeta),$$

which already follows from [1], Theorem I.4.1.

REFERENCES

[1] Ph. Cassou-Noguès and M. J. Taylor, *Elliptic Functions and Rings of Integers*, Progr. Math. 66, Birkhäuser, 1987.

[2] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Ergeb. Math. (3) 1, Springer, 1983.

[3] R. Massy, *Bases normales d'entiers relatives quadratiques*, J. Number Theory 38 (1991), 216–239.

[4] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer, 1990.

[5] K. W. Roggenkamp and M. J. Taylor, *Group Rings and Class Groups*, DMV Sem. 18, Birkhäuser, 1992.
[6] M. J. Taylor, *Relative Galois module structure of rings of integers*, in: Orders and their Applications (Proc. Oberwolfach 1984), I. Reiner and K. W. Roggenkamp (eds.), Lecture Notes in Math. 1142, Springer, 1985, 289–306.

INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
HEINRICHSTR. 36
A-8010 GRAZ, ÖSTERREICH

Reçu par la Rédaction le 7.7.1993